Interfacce logiche (LIF)

ONTAP 9

NetApp
February 06, 2026

Sommario

Interfacce logiche (LIF) . . . 1
- Panoramica della LIF . . . 1
  - Scopri la configurazione LIF per un cluster ONTAP . . . 1
  - Informazioni sulla compatibilità delle LIF ONTAP con i tipi di porte . . . 3
  - Ruoli e policy di servizio LIF supportati per la tua versione ONTAP . . . 4
  - Scopri le LIF e le policy di servizio di ONTAP . . . 5
- Gestire le LIF . . . 10
  - Configurazione delle policy di servizio LIF per un cluster ONTAP . . . 10
  - Crea LIF ONTAP . . . 16
  - Modificare le LIF ONTAP . . . 22
  - Migrazione delle LIF ONTAP . . . 24
  - Ripristina una LIF nella porta home dopo un failover di un nodo ONTAP o una migrazione delle porte . . . 27
  - Recupera una LIF ONTAP configurata in modo errato . . . 27
  - Eliminare le LIF ONTAP . . . 29
- Configurare la LIF ONTAP Virtual IP (VIP) . . . 29
  - Impostazione del protocollo Border gateway (BGP) . . . 30
  - Creare una LIF di dati IP (VIP) virtuale . . . 34
  - Comandi per la gestione del BGP . . . 35

Interfacce logiche (LIF)

Panoramica della LIF

Scopri la configurazione LIF per un cluster ONTAP

Una LIF (interfaccia logica) rappresenta un punto di accesso di rete a un nodo del cluster. È possibile configurare le LIF sulle porte su cui il cluster invia e riceve le comunicazioni sulla rete.

Un amministratore del cluster può creare, visualizzare, modificare, migrare, ripristinare, Oppure eliminare i LIF. Un amministratore di SVM può visualizzare solo le LIF associate a SVM.

Un LIF è un indirizzo IP o WWPN con caratteristiche associate, ad esempio una policy di servizio, una porta home, un nodo home, un elenco di porte a cui eseguire il failover e una policy firewall. È possibile configurare le LIF sulle porte su cui il cluster invia e riceve le comunicazioni sulla rete.

> A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere "Configurare le policy firewall per le LIF".

Le LIF possono essere ospitate sulle seguenti porte:

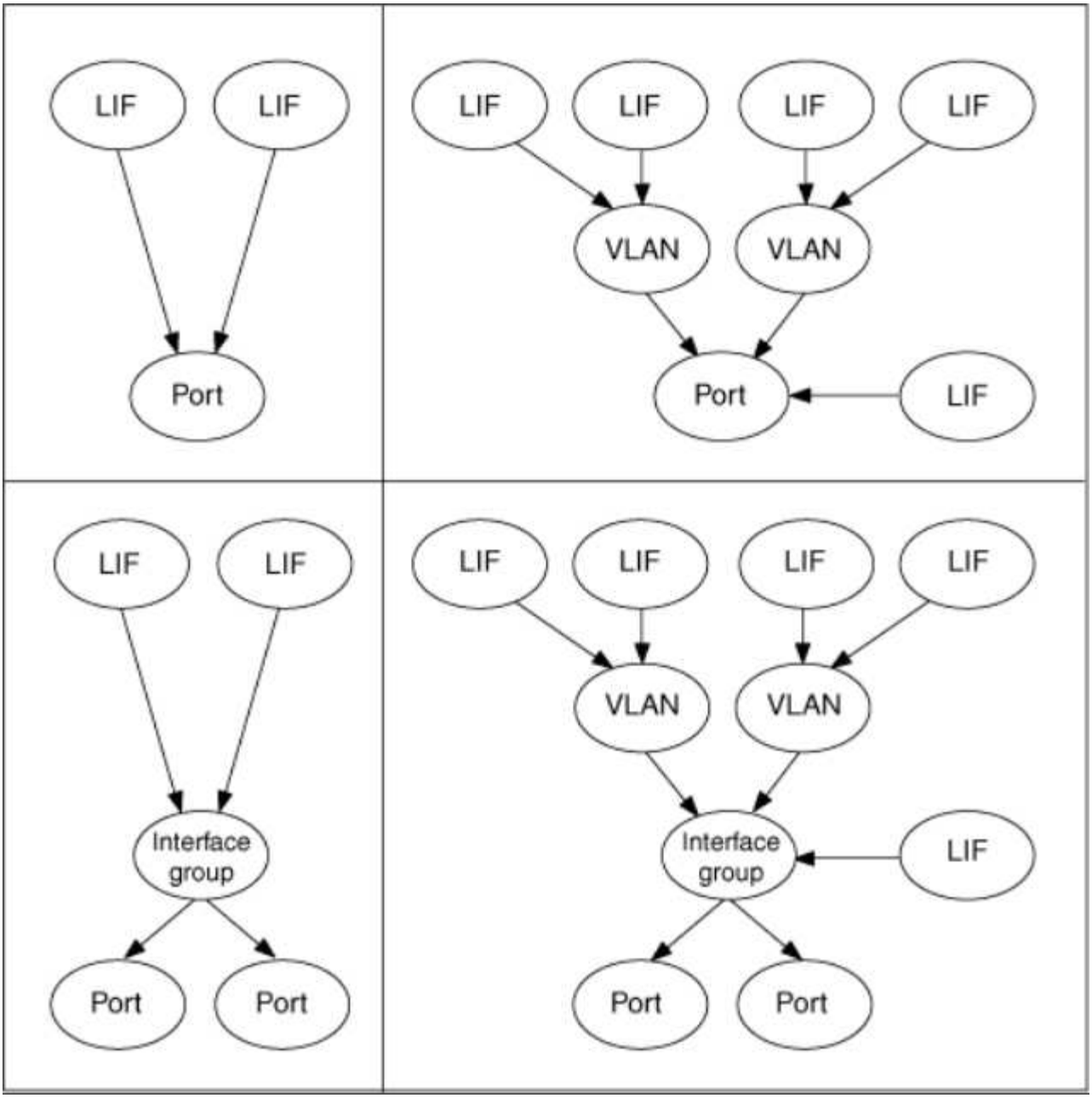
- Porte fisiche che non fanno parte di gruppi di interfacce
- Gruppi di interfacce
- VLAN
- Porte fisiche o gruppi di interfacce che ospitano VLAN
- Porte VIP (Virtual IP)

  A partire da ONTAP 9.5, le LIF VIP sono supportate e sono ospitate su porte VIP.

Durante la configurazione di protocolli SAN come FC su un LIF, questo verrà associato a un WWPN.

"Amministrazione SAN"

La seguente figura illustra la gerarchia di porte in un sistema ONTAP:



Failover e sconto della LIF

Un failover LIF si verifica quando una LIF passa dal nodo home o dalla porta al nodo partner ha o alla porta. Il failover di una LIF può essere attivato automaticamente da ONTAP o manualmente dall'amministratore del cluster per determinati eventi, come un collegamento Ethernet fisico inattivo o un nodo che abbandona il quorum del database replicato (RDB). Quando si verifica un failover della LIF, ONTAP continua a lavorare normalmente sul nodo partner fino alla risoluzione della causa del failover. Quando il nodo home o la porta torna in salute, la LIF viene riportata dal partner di ha al nodo home o alla porta. Questa inversione è chiamata sconto.

Per il failover e il giveback della LIF, le porte di ciascun nodo devono appartenere allo stesso dominio di broadcast. Per verificare che le porte rilevanti su ciascun nodo appartengano allo stesso dominio di broadcast, vedere quanto segue:

- ONTAP 9,8 e versioni successive: "Riparare la raggiungibilità delle porte"

- ONTAP 9,7 e versioni precedenti: "Aggiungere o rimuovere porte da un dominio di broadcast"

Per le LIF con failover LIF abilitato (automaticamente o manualmente) si applica quanto segue:

- Per le LIF che utilizzano una policy di servizio dati, puoi controllare le restrizioni delle policy di failover:
  - ONTAP 9,6 e versioni successive: "LIF e policy di servizio in ONTAP 9.6 e versioni successive"
  - ONTAP 9,5 e versioni precedenti: "Ruoli LIF in ONTAP 9.5 e versioni precedenti"
- L'autorevert dei LIF avviene quando l'autorevert è impostato su `true` E quando la porta home della LIF è in buone condizioni e in grado di ospitare la LIF.
- In un takeover pianificato o non pianificato del nodo, la LIF sul nodo preso in consegna, esegue il failover nel partner di ha. La porta su cui si verifica il failover di LIF è determinata da VIF Manager.
- Una volta completato il failover, la LIF funziona normalmente.
- Al momento di eseguire un giveback, la LIF torna al nodo home e alla porta, se l'opzione di indirizzamento automatico è impostata su `true`.
- Quando un collegamento ethernet si interrompe su una porta che ospita una o più LIF, VIF Manager esegue la migrazione delle LIF dalla porta inattiva a una porta diversa nello stesso dominio di trasmissione. La nuova porta potrebbe trovarsi nello stesso nodo o nel suo partner ha. Dopo il ripristino del collegamento e se l'opzione di ripristino automatico è impostata su `true`, Il VIF Manager riporta le LIF al loro nodo principale e alla loro porta principale.
- Quando un nodo abbandona il quorum del database replicato (RDB), il VIF Manager migra le LIF dal nodo fuori quorum al partner ha. Dopo che il nodo torna al quorum e se l'opzione di revert automatico è impostata su `true`, Il VIF Manager riporta le LIF al loro nodo principale e alla loro porta principale.

Informazioni sulla compatibilità delle LIF ONTAP con i tipi di porte

Le LIF possono avere caratteristiche diverse per supportare diversi tipi di porta.

> Quando le LIF di intercluster e di gestione sono configurate nella stessa subnet, il traffico di gestione potrebbe essere bloccato da un firewall esterno e le connessioni AutoSupport e NTP potrebbero non funzionare. È possibile ripristinare il sistema eseguendo `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` Comando per attivare/disattivare la LIF dell'intercluster. Tuttavia, è necessario impostare la LIF di intercluster e la LIF di gestione in diverse subnet per evitare questo problema.

LIF	Descrizione
LIF dati	LIF associata a una macchina virtuale di storage (SVM) e utilizzata per comunicare con i client. Su una porta è possibile disporre di più LIF di dati. Queste interfacce possono migrare o eseguire il failover in tutto il cluster. È possibile modificare una LIF dei dati per fungere da LIF di gestione SVM modificando la relativa policy firewall in mgmt. Le sessioni stabilite per i server NIS, LDAP, Active Directory, WINS e DNS utilizzano le LIF dei dati.

LIF del cluster	LIF utilizzata per trasportare il traffico intracluster tra i nodi di un cluster. Le LIF del cluster devono sempre essere create sulle porte del cluster. Le LIF del cluster possono eseguire il failover tra le porte del cluster sullo stesso nodo, ma non possono essere migrate o sottoposte a failover su un nodo remoto. Quando un nuovo nodo si unisce a un cluster, gli indirizzi IP vengono generati automaticamente. Tuttavia, se si desidera assegnare manualmente gli indirizzi IP alle LIF del cluster, è necessario assicurarsi che i nuovi indirizzi IP si trovino nello stesso intervallo di subnet delle LIF del cluster esistenti.
LIF gestione cluster	LIF che fornisce un'unica interfaccia di gestione per l'intero cluster. Una LIF di gestione del cluster può eseguire il failover su qualsiasi nodo del cluster. Non è possibile eseguire il failover sulle porte del cluster o dell'intercluster
LIF intercluster	Una LIF utilizzata per la comunicazione tra cluster, il backup e la replica. È necessario creare una LIF intercluster su ciascun nodo del cluster prima di stabilire una relazione di peering del cluster. Queste LIF possono eseguire il failover solo sulle porte dello stesso nodo. Non è possibile eseguire la migrazione o il failover su un altro nodo del cluster.
LIF di gestione dei nodi	LIF che fornisce un indirizzo IP dedicato per la gestione di un nodo specifico in un cluster. Le LIF di gestione dei nodi vengono create al momento della creazione o dell'adesione al cluster. Queste LIF vengono utilizzate per la manutenzione del sistema, ad esempio quando un nodo diventa inaccessibile dal cluster.
LIF. VIP	Per LIF VIP si intende qualsiasi LIF di dati creata su una porta VIP. Per ulteriori informazioni, vedere "Configurare i LIF VIP (Virtual IP)".

Informazioni correlate

- "modifica dell'interfaccia di rete"

Ruoli e policy di servizio LIF supportati per la tua versione ONTAP

Con il passare del tempo, il modo in cui ONTAP gestisce il tipo di traffico supportato dalle LIF è cambiato.

- Le versioni ONTAP 9.5 e precedenti utilizzano i ruoli LIF e i servizi firewall.
- ONTAP 9.6 e versioni successive utilizzano i criteri di servizio LIF:
  - La versione ONTAP 9.5 ha introdotto le politiche di servizio LIF.
  - ONTAP 9.6 ha sostituito i ruoli LIF con le politiche di servizio LIF.
  - ONTAP 9.10,1 ha sostituito i servizi firewall con le policy di servizio LIF.

Il metodo configurato dipende dal rilascio di ONTAP in uso.

Ulteriori informazioni su:

- Criteri firewall, fare riferimento a "Comando: Firewall-policy-show".
- I ruoli LIF, fare riferimento alla "Ruoli LIF (ONTAP 9,5 e versioni precedenti)".
- Le policy di servizio LIF, fare riferimento alla "LIF e policy di servizio (ONTAP 9,6 e versioni successive)".

Scopri le LIF e le policy di servizio di ONTAP

È possibile assegnare policy di servizio (invece di ruoli LIF o policy firewall) alle LIF che determinano il tipo di traffico supportato per le LIF. Le policy di servizio definiscono una raccolta di servizi di rete supportati da una LIF. ONTAP offre una serie di policy di servizio integrate che possono essere associate a una LIF.

Il metodo di gestione del traffico di rete è diverso in ONTAP 9,7 e nelle versioni precedenti. Se è necessario gestire il traffico su una rete con ONTAP 9,7 e versioni precedenti, fare riferimento alla "Ruoli LIF (ONTAP 9,5 e versioni precedenti)".

I protocolli FCP e NVMe/FCP attualmente non richiedono una service-policy.

È possibile visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando: `network interface service-policy show`

Ulteriori informazioni su `network interface service-policy show` nella "Riferimento al comando ONTAP".

Le funzioni non associate a un servizio specifico utilizzeranno un comportamento definito dal sistema per selezionare le LIF per le connessioni in uscita.

Le applicazioni in una LIF con una politica di servizio vuota potrebbero comportarsi in modo imprevisto.

Policy di servizio per SVM di sistema

La SVM amministrativa e qualsiasi SVM di sistema contengono policy di servizio che possono essere utilizzate per le LIF in tale SVM, incluse le LIF di gestione e intercluster. Questi criteri vengono creati automaticamente dal sistema quando viene creato un IPSpace.

Nella tabella seguente sono elencate le policy integrate per le LIF nelle SVM di sistema a partire da ONTAP 9.12.1. Per le altre release, visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando:

```
network interface service-policy show
```

Policy	Servizi inclusi	Ruolo equivalente	Descrizione
intercluster predefinito	intercluster-core, management-https	intercluster	Utilizzato da LIF che trasportano traffico intercluster. Nota: Service Intercluster-core è disponibile da ONTAP 9.5 con il nome net-intercluster service policy.
default-route-announce	gestione-bgp	-	Utilizzato da LIF con connessioni peer BGP Nota: Disponibile da ONTAP 9.5 con il nome net-route-announce service policy.

gestione predefinita	management-core, management-https, management-http, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-forwarding	node-mgmt, o cluster-mgmt	Utilizzare questa policy di gestione con ambito di sistema per creare LIF di gestione con ambito di nodo e cluster di proprietà di una SVM di sistema. Queste LIF possono essere utilizzate per le connessioni in uscita verso server DNS, ad, LDAP o NIS, nonché per alcune connessioni aggiuntive per supportare le applicazioni eseguite per conto dell'intero sistema. A partire da ONTAP 9.12.1, puoi usare il `management-log-forwarding` servizio per controllare le LIF che vengono utilizzate per inoltrare i log di audit a un server syslog remoto.

Nella tabella seguente sono elencati i servizi che le LIF possono utilizzare in una SVM di sistema a partire da ONTAP 9.11.1:

Servizio	Limiti di failover	Descrizione
core intercluster	solo nodo principale	Servizi di intercluster principali
core di gestione	-	Servizi di gestione principali
gestione-ssh	-	Servizi per l'accesso alla gestione SSH
gestione-http	-	Servizi per l'accesso alla gestione HTTP
gestione-https	-	Servizi per l'accesso alla gestione HTTPS
gestione: autosupport	-	Servizi relativi alla pubblicazione dei payload AutoSupport
gestione-bgp	solo porta home	Servizi correlati alle interazioni peer BGP
backup-ndmp-control	-	Servizi per i controlli di backup NDMP
gestione-ems	-	Servizi per l'accesso alla messaggistica di gestione
client ntp di gestione	-	Introdotto in ONTAP 9.10.1. Servizi per l'accesso al client NTP.
management-ntp-server	-	Introdotto in ONTAP 9.10.1. Servizi per l'accesso alla gestione del server NTP
gestione-portmap	-	Servizi per la gestione di portmap

management-rsh-server	-	Servizi per la gestione dei server rsh
server-snmp-di-gestione	-	Servizi per la gestione del server SNMP
management-telnet-server	-	Servizi per la gestione dei server telnet
management-log-forwarding	-	Introdotto in ONTAP 9.12.1. Servizi per l'inoltro dei log di controllo

Policy di servizio per SVM di dati

Tutti i dati SVM contengono policy di servizio che possono essere utilizzate dai LIF in tale SVM.

Nella tabella seguente sono elencate le policy integrate per le LIF in SVM di dati a partire da ONTAP 9.11.1. Per le altre release, visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando:

```
network interface service-policy show
```

Policy	Servizi inclusi	Protocollo dati equivalente	Descrizione
gestione predefinita	data-core, management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-client-ldap, management-nis-client	nessuno	Utilizza questa policy di gestione con ambito SVM per creare LIF di gestione SVM di proprietà di una SVM di dati. Queste LIF possono essere utilizzate per fornire l'accesso SSH o HTTPS agli amministratori di SVM. Se necessario, questi LIF possono essere utilizzati per le connessioni in uscita a server DNS, ad, LDAP o NIS esterni.
blocchi-di-dati-predefiniti	data-core, data-iscsi	iscsi	Utilizzato da LIF che trasportano traffico dati SAN orientato a blocchi. A partire da ONTAP 9.10.1, la policy "default-data-blocks" è obsoleta. Utilizzare invece la policy di servizio "default-data-iscsi".
default-data-files	data-core, data-fpolicy-client, data-dns-server, data-FlexCache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Utilizzare il criterio default-data-files per creare LIF NAS che supportino protocolli di dati basati su file. A volte è presente un solo LIF nella SVM, pertanto questo criterio consente di utilizzare la LIF per le connessioni in uscita a un server DNS, ad, LDAP o NIS esterno. È possibile rimuovere questi servizi da questa policy se si preferisce che queste connessioni utilizzino solo LIF di gestione.

default-data-iscsi	data-core, data-iscsi	iscsi	Utilizzato da LIF che trasportano traffico dati iSCSI.
default-data-nvme-tcp	data-core, data-nvme-tcp	nvme-tcp	Utilizzato da LIF che trasportano traffico dati NVMe/TCP.

La tabella seguente elenca i servizi che possono essere utilizzati su una SVM dati insieme alle eventuali restrizioni imposte da ogni servizio alla policy di failover di una LIF a partire da ONTAP 9.11.1:

Servizio	Restrizioni di failover	Descrizione
gestione-ssh	-	Servizi per l'accesso alla gestione SSH
gestione-http	-	Introdotto nei servizi ONTAP 9.10.1 per l'accesso alla gestione HTTP
gestione-https	-	Servizi per l'accesso alla gestione HTTPS
gestione-portmap	-	Servizi per l'accesso alla gestione di portmap
server-snmp-di-gestione	-	Introdotto nei servizi ONTAP 9.10.1 per l'accesso alla gestione del server SNMP
core di dati	-	Servizi dati principali
nfs dati	-	Servizio dati NFS
cifs dei dati	-	Servizio dati CIFS
data-flexcache	-	Servizio dati FlexCache
iscsi dati	home-port-only per AFF/FAS; sfo-partner-only per ASA	Servizio dati iSCSI
backup-ndmp-control	-	Introdotto in ONTAP 9.10.1 Backup NDMP controlla il servizio dati
server-dns-dati	-	Introdotto nel servizio dati del server DNS di ONTAP 9.10.1
data-fpolicy-client	-	Servizio dati delle policy di screening dei file
data-nvme-tcp	solo porta home	Introdotto nel servizio dati TCP NVMe di ONTAP 9.10.1

data-s3-server	-	Servizio dati server Simple Storage Service (S3)

È necessario conoscere il modo in cui le policy di servizio vengono assegnate alle LIF nelle SVM di dati:

- Se viene creata una SVM dati con un elenco di servizi dati, le policy di servizio "default-data-files" e "default-data-block" incorporate in tale SVM vengono create utilizzando i servizi specificati.
- Se viene creata una SVM dati senza specificare un elenco di servizi dati, le policy di servizio "default-data-files" e "default-data-block" incorporate in tale SVM vengono create utilizzando un elenco predefinito di servizi dati.

  L'elenco dei servizi dati predefiniti include i servizi iSCSI, NFS, NVMe, SMB e FlexCache.

- Quando si crea una LIF con un elenco di protocolli dati, una politica di servizio equivalente ai protocolli dati specificati viene assegnata alla LIF.
- Se non esiste una politica di servizio equivalente, viene creata una politica di servizio personalizzata.
- Quando si crea una LIF senza una policy di servizio o un elenco di protocolli dati, la policy di servizio default-data-files viene assegnata alla LIF per impostazione predefinita.

Servizio data-core

Il servizio data-core consente ai componenti che in precedenza utilizzavano le LIF con il ruolo dati di funzionare come previsto sui cluster che sono stati aggiornati per gestire le LIF utilizzando le policy di servizio invece dei ruoli LIF (che sono deprecati in ONTAP 9.6).

La specifica del data-core come servizio non apre alcuna porta nel firewall, ma il servizio deve essere incluso in qualsiasi politica di servizio in una SVM dati. Ad esempio, per impostazione predefinita, la politica di servizio file di dati predefiniti contiene i seguenti servizi:

- core di dati
- nfs dati
- cifs dei dati
- data-flexcache

Il servizio data-core deve essere incluso nella policy per garantire che tutte le applicazioni che utilizzano LIF funzionino come previsto, ma gli altri tre servizi possono essere rimossi, se lo si desidera.

Servizio LIF lato client

A partire da ONTAP 9.10.1, ONTAP offre servizi LIF lato client per più applicazioni. Questi servizi consentono di controllare quali LIF vengono utilizzati per le connessioni in uscita per conto di ciascuna applicazione.

I seguenti nuovi servizi consentono agli amministratori di controllare quali LIF vengono utilizzati come indirizzi di origine per determinate applicazioni.

Servizio	Restrizioni SVM	Descrizione
management-ad-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client Active Directory per le connessioni in uscita a un server ad esterno.

client-dns-di-gestione	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client DNS per le connessioni in uscita a un server DNS esterno.
management-ldap-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client LDAP per le connessioni in uscita a un server LDAP esterno.
management-nis-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client NIS per le connessioni in uscita a un server NIS esterno.
client ntp di gestione	solo sistema	A partire da ONTAP 9.10.1, ONTAP fornisce il servizio client NTP per le connessioni in uscita a un server NTP esterno.
data-fpolicy-client	solo dati	A partire da ONTAP 9.8, ONTAP fornisce il servizio client per le connessioni FPolicy in uscita.

Ciascuno dei nuovi servizi viene incluso automaticamente in alcune policy di servizio integrate, ma gli amministratori possono rimuoverli dalle policy integrate o aggiungerli a policy personalizzate per controllare quali LIF vengono utilizzate per le connessioni in uscita per conto di ciascuna applicazione.

Informazioni correlate

- "visualizzazione della politica di servizio dell'interfaccia di rete"

Gestire le LIF

Configurazione delle policy di servizio LIF per un cluster ONTAP

È possibile configurare le policy di servizio LIF per identificare un singolo servizio o un elenco di servizi che utilizzeranno una LIF.

Creare una politica di servizio per le LIF

È possibile creare una politica di servizio per le LIF. È possibile assegnare una policy di servizio a una o più LIF, consentendo così al LIF di trasportare il traffico per un singolo servizio o un elenco di servizi.

Per eseguire, sono necessari privilegi avanzati `network interface service-policy create` comando.

A proposito di questa attività

I servizi integrati e le policy di servizio sono disponibili per la gestione del traffico di dati e di gestione su SVM di dati e di sistema. La maggior parte dei casi di utilizzo è soddisfatta utilizzando una politica di servizio integrata piuttosto che creare una politica di servizio personalizzata.

Se necessario, è possibile modificare queste policy di servizio incorporate.

Fasi

1. Visualizzare i servizi disponibili nel cluster:

```
network interface service show
```

I servizi rappresentano le applicazioni a cui si accede da una LIF e le applicazioni servite dal cluster. Ogni servizio include zero o più porte TCP e UDP su cui l'applicazione è in ascolto.

Sono disponibili i seguenti servizi di gestione e dati aggiuntivi:

```
cluster1::> network interface service show

Service                     Protocol:Ports
-------                     --------------
cluster-core                -
data-cifs                   -
data-core                   -
data-flexcache              -
data-iscsi                  -
data-nfs                    -
intercluster-core           tcp:11104-11105
management-autosupport      -
management-bgp              tcp:179
management-core             -
management-https            tcp:443
management-ssh              tcp:22
12 entries were displayed.
```

2. Visualizzare le policy di servizio esistenti nel cluster:

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. Creare una politica di servizio:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- "nome_servizio" specifica un elenco di servizi da includere nella policy.
- "IP_address/mask" specifica l'elenco di subnet mask per gli indirizzi ai quali è consentito l'accesso ai servizi nella politica di servizio. Per impostazione predefinita, tutti i servizi specificati vengono aggiunti con un elenco di indirizzi consentiti predefinito di 0.0.0.0/0, che consente il traffico da tutte le subnet. Quando viene fornito un elenco di indirizzi non predefinito, i file LIF che utilizzano il criterio sono configurati per bloccare tutte le richieste con un indirizzo di origine che non corrisponde a nessuna delle maschere specificate.

  Nell'esempio seguente viene illustrato come creare una policy del servizio dati, *svm1_data_policy*, per una SVM che include i servizi *NFS* e *SMB*:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

  Nell'esempio seguente viene illustrato come creare una policy di servizio tra cluster:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. Verificare che la politica di servizio sia stata creata.

```
cluster1::> network interface service-policy show
```

   Il seguente output mostra le policy di servizio disponibili:

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
--------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

Al termine

Assegnare la politica di servizio a una LIF al momento della creazione o modificando una LIF esistente.

Assegnare una politica di servizio a una LIF

È possibile assegnare una politica di servizio a una LIF al momento della creazione della LIF o modificando la LIF. Una politica di servizio definisce l'elenco dei servizi che possono essere utilizzati con LIF.

A proposito di questa attività

È possibile assegnare le policy di servizio per le LIF nelle SVM di amministrazione e dati.

Fase

A seconda del momento in cui si desidera assegnare la politica di servizio a una LIF, eseguire una delle seguenti operazioni:

Se sei…	Assegnare la politica di servizio…
Creazione di una LIF	Interfaccia di rete create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> {(-address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
Modifica di una LIF	modifica interfaccia di rete -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

Quando si specifica una politica di servizio per una LIF, non è necessario specificare il protocollo dati e il ruolo per la LIF. È supportata anche la creazione di LIF specificando il ruolo e i protocolli dati.

> Una politica di servizio può essere utilizzata solo dalle LIF nella stessa SVM specificata durante la creazione della politica di servizio.

Esempi

Nell'esempio seguente viene illustrato come modificare la politica di servizio di una LIF per utilizzare la politica di servizio di gestione predefinita:

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

Comandi per la gestione delle policy di servizio LIF

Utilizzare `network interface service-policy` Comandi per gestire le policy di servizio LIF.

Ulteriori informazioni su `network interface service-policy` nella "Riferimento al comando ONTAP".

Prima di iniziare

La modifica della policy di servizio di una LIF in una relazione di SnapMirror attiva interrompe il programma di replica. Se si converte una LIF da intercluster a non intercluster (o viceversa), le modifiche non verranno replicate nel cluster sottoposto a peering. Per aggiornare il cluster peer dopo aver modificato la policy di servizio LIF, eseguire prima l' `snapmirror abort` operazione quindi risincronizzazione della relazione di replica.

Se si desidera…	Utilizzare questo comando…
Creazione di una politica di servizio (sono richiesti privilegi avanzati)	`network interface service-policy create`
Aggiunta di una voce di servizio aggiuntiva a una policy di servizio esistente (sono richiesti privilegi avanzati)	`network interface service-policy add-service`
Clonare una policy di servizio esistente (sono richiesti privilegi avanzati)	`network interface service-policy clone`
Modifica di una voce di servizio in una policy di servizio esistente (sono richiesti privilegi avanzati)	`network interface service-policy modify-service`
Rimozione di una voce di servizio da una policy di servizio esistente (sono richiesti privilegi avanzati)	`network interface service-policy remove-service`
Rinominare una policy di servizio esistente (sono richiesti privilegi avanzati)	`network interface service-policy rename`
Eliminazione di una policy di servizio esistente (privilegi avanzati richiesti)	`network interface service-policy delete`
Ripristinare una policy di servizio integrata al suo stato originale (sono richiesti privilegi avanzati)	`network interface service-policy restore-defaults`
Visualizzare le policy di servizio esistenti	`network interface service-policy show`

Informazioni correlate

- "mostra servizio interfaccia di rete"
- "politica di servizio dell'interfaccia di rete"
- "interruzione snapmirror"

Crea LIF ONTAP

Una SVM fornisce i dati ai client attraverso una o più interfacce logiche di rete (LIF). Per accedere ai dati, è necessario creare LIF sulle porte che si desidera utilizzare. Una LIF (interfaccia di rete) è un indirizzo IP associato a una porta fisica o logica. In caso di guasto di un componente, una LIF può eseguire il failover o essere migrata su una porta fisica diversa, continuando così a comunicare con la rete.

Best practice

Le porte dello switch connesse a ONTAP devono essere configurate come porte edge spanning-tree per ridurre i ritardi durante la migrazione LIF.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- La porta di rete fisica o logica sottostante deve essere stata configurata con lo stato di attivazione amministrativa.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

  Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando System Manager o `network subnet create` comando.

  Ulteriori informazioni su `network subnet create` nella "Riferimento al comando ONTAP".

- Il meccanismo per specificare il tipo di traffico gestito da una LIF è stato modificato. Per ONTAP 9.5 e versioni precedenti, i LIF utilizzavano i ruoli per specificare il tipo di traffico che gestirebbe. A partire da ONTAP 9.6, le LIF utilizzano le policy di servizio per specificare il tipo di traffico che gestirebbe.

A proposito di questa attività

- Non è possibile assegnare protocolli NAS e SAN allo stesso LIF.

  I protocolli supportati sono SMB, NFS, FlexCache, iSCSI e FC; ISCSI e FC non possono essere combinati con altri protocolli. Tuttavia, i protocolli SAN basati su NAS ed Ethernet possono essere presenti sulla stessa porta fisica.

  - Non si consiglia di configurare le LIF che trasportano il traffico SMB in modo da ripristinare automaticamente i propri nodi domestici. Questo suggerimento è obbligatorio se il server SMB deve ospitare una soluzione per operazioni senza interruzioni con Hyper-V o SQL Server su SMB.
- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Tutti i servizi di mappatura dei nomi e risoluzione dei nomi host utilizzati da una SVM, come DNS, NIS, LDAP e Active Directory, Deve essere raggiungibile da almeno un LIF che gestisce il traffico dati della SVM.
- Una LIF che gestisce il traffico intracluster tra i nodi non deve trovarsi sulla stessa subnet di una LIF che gestisce il traffico di gestione o di una LIF che gestisce il traffico di dati.
- La creazione di una LIF che non dispone di una destinazione di failover valida genera un messaggio di avviso.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster:
  - System Manager: A partire da ONTAP 9.12.0, visualizzare il throughput nella griglia dell'interfaccia di rete.
  - CLI: Utilizzare `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).

    Ulteriori informazioni su `network interface capacity show` e `network interface capacity details show` nella "Riferimento al comando ONTAP".

- A partire da ONTAP 9.7, se sono già presenti altre LIF per la SVM nella stessa sottorete, non è necessario specificare la porta home della LIF. ONTAP sceglie automaticamente una porta casuale sul nodo principale specificato nello stesso dominio di trasmissione delle altre LIF già configurate nella stessa sottorete.

  A partire da ONTAP 9.4, FC-NVMe è supportato. Se si sta creando una LIF FC-NVMe, tenere presente quanto segue:

    - Il protocollo NVMe deve essere supportato dall'adattatore FC su cui viene creato il LIF.
    - FC-NVMe può essere l'unico protocollo dati sulle LIF dei dati.
- È necessario configurare un LIF che gestisca il traffico di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.
- Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
- È possibile configurare un massimo di due LIF NVMe che gestiscono il traffico dati per SVM, per nodo.
- Quando si crea un'interfaccia di rete con una subnet, ONTAP seleziona automaticamente un indirizzo IP disponibile dalla subnet selezionata e lo assegna all'interfaccia di rete. È possibile modificare la subnet se sono presenti più subnet, ma non è possibile modificare l'indirizzo IP.
- Quando si crea (aggiunge) una SVM per un'interfaccia di rete, non è possibile specificare un indirizzo IP compreso nell'intervallo di una subnet esistente. Viene visualizzato un errore di conflitto di subnet. Questo problema si verifica in altri flussi di lavoro per un'interfaccia di rete, come la creazione o la modifica di interfacce di rete tra cluster nelle impostazioni SVM o nelle impostazioni del cluster.
- A partire da ONTAP 9.10.1, i `network interface` comandi CLI includono un `-rdma-protocols` parametro per le configurazioni NFS su RDMA. La creazione di interfacce di rete per le configurazioni NFS su RDMA è supportata in System Manager a partire da ONTAP 9.12.1. Per ulteriori informazioni, vedere Configurare LIFS per NFS su RDMA.
- A partire da ONTAP 9.11.1, il failover automatico iSCSI LIF è disponibile nelle piattaforme ASA (All-Flash SAN Array).

  Il failover LIF iSCSI viene attivato automaticamente (il criterio di failover è impostato su `sfo-partner-only` e il valore di autorevert è impostato su `true`) Sulle LIF iSCSI appena create se non esistono LIF iSCSI nella SVM specificata o se tutte le LIF iSCSI esistenti nella SVM specificata sono già abilitate con il failover LIF iSCSI.

  Se dopo aver eseguito l'aggiornamento a ONTAP 9.11.1 o versioni successive si dispone di LIF iSCSI esistenti in una SVM che non sono state abilitate con la funzione di failover LIF iSCSI e si creano nuove LIF iSCSI nella stessa SVM, le nuove LIF iSCSI assumono la stessa policy di failover (`disabled`) Delle LIF iSCSI esistenti in SVM.

  "Failover LIF iSCSI per piattaforme ASA"

A partire da ONTAP 9.7, ONTAP sceglie automaticamente la porta home di un LIF, purché almeno un LIF esista già nella stessa sottorete di tale LIF. ONTAP sceglie una porta home nello stesso dominio di broadcast delle altre LIF della subnet. È comunque possibile specificare una porta home, ma non è più necessaria (a meno che non esistano file LIF in tale subnet nell'IPSpace specificato).

A partire da ONTAP 9.12.0, la procedura da seguire dipende dall'interfaccia in uso: Gestore di sistema o CLI:

System Manager

Utilizzare System Manager per aggiungere un'interfaccia di rete

Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare + Add .
3. Selezionare uno dei seguenti ruoli di interfaccia:
   a. Dati
   b. Intercluster
   c. Gestione SVM
4. Selezionare il protocollo:
   a. SMB/CIFS E NFS
   b. ISCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. Assegnare un nome al LIF o accettare il nome generato dalle selezioni precedenti.
6. Accettare il nodo home o utilizzare il menu a discesa per selezionarlo.
7. Se almeno una subnet è configurata nell'IPSpace dell'SVM selezionato, viene visualizzato il menu a discesa Subnet (sottorete).
   a. Se si seleziona una subnet, selezionarla dall'elenco a discesa.
   b. Se si procede senza una subnet, viene visualizzato il menu a discesa del dominio di trasmissione:
      i. Specificare l'indirizzo IP. Se l'indirizzo IP è in uso, viene visualizzato un messaggio di avviso.
      ii. Specificare una subnet mask.
8. Selezionare la porta home dal dominio di trasmissione, automaticamente (scelta consigliata) o selezionandola dal menu a discesa. Il controllo della porta Home viene visualizzato in base al dominio di trasmissione o alla selezione della subnet.
9. Salvare l'interfaccia di rete.

CLI

Utilizzare la CLI per creare una LIF

Fasi

1. Determinare quali porte del dominio di trasmissione si desidera utilizzare per la LIF.

   ```
   network port broadcast-domain show -ipspace ipspace1
   ```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

Ulteriori informazioni su `network port broadcast-domain show` nella "Riferimento al comando ONTAP".

2. Verificare che la subnet che si desidera utilizzare per i file LIF contenga un numero sufficiente di indirizzi IP inutilizzati.

   `network subnet show -ipspace ipspace1`

   Ulteriori informazioni su `network subnet show` nella "Riferimento al comando ONTAP".

3. Creare una o più LIF sulle porte che si desidera utilizzare per accedere ai dati.

   NetApp consiglia di creare oggetti subnet per tutte le LIF sulle SVM di dati. Ciò è particolarmente importante per le configurazioni MetroCluster, in cui l'oggetto subnet consente a ONTAP di determinare le destinazioni di failover sul cluster di destinazione poiché ogni oggetto subnet ha un dominio broadcast associato. Per istruzioni, fare riferimento alla "Creare una subnet".

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - `-home-node` È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

     Puoi anche specificare se LIF deve ripristinare automaticamente il nodo home e la porta home con l'opzione -auto-revert.

   Ulteriori informazioni su `network interface revert` nella "Riferimento al comando ONTAP".

   - `-home-port` È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
   - È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.
   - Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene

automaticamente aggiunto un percorso predefinito a tale gateway.

- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Ulteriori informazioni su `network route create` nella "Riferimento al comando ONTAP".
- `-auto-revert` Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `true` in base alle policy di gestione della rete nel proprio ambiente.
- `-service-policy` A partire da ONTAP 9.5, è possibile assegnare una politica di servizio per la LIF con `-service-policy` opzione. Quando viene specificata una policy di servizio per una LIF, questa viene utilizzata per creare un ruolo predefinito, una policy di failover e un elenco di protocolli dati per la LIF. In ONTAP 9.5, le policy di servizio sono supportate solo per i servizi peer di intercluster e BGP. In ONTAP 9.6, è possibile creare policy di servizio per diversi servizi di gestione e dati.
- `-data-protocol` Consente di creare una LIF che supporti i protocolli FCP o NVMe/FC. Questa opzione non è necessaria quando si crea un LIF IP.

4. **Opzionale**: Assegnare un indirizzo IPv6 nell'opzione -address:

   a. Utilizzare `network ndp prefix show` Per visualizzare l'elenco dei prefissi RA appresi su varie interfacce.

      Il `network ndp prefix show` il comando è disponibile a livello di privilegio avanzato.

      Ulteriori informazioni su `network ndp prefix show` nella "Riferimento al comando ONTAP".

   b. Utilizzare il formato `prefix::id` Per costruire manualmente l'indirizzo IPv6.

      `prefix` è il prefisso appreso sulle varie interfacce.

   Per derivare il `id`, scegliere un numero esadecimale casuale a 64 bit.

5. Verificare che la configurazione dell'interfaccia LIF sia corretta.

   ```
   network interface show -vserver vs1
   ```

   ```
             Logical    Status     Network          Current   Current Is
   Vserver   Interface  Admin/Oper Address/Mask     Node      Port
   Home
   --------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
              lif1       up/up      10.0.0.128/24    node1     e0d
   true
   ```

   Ulteriori informazioni su `network interface show` nella "Riferimento al comando ONTAP".

6. Verificare che la configurazione del gruppo di failover sia quella desiderata.

```
network interface show -failover -vserver vs1
```

```
         Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un…	Utilizzare…
Indirizzo IPv4	ping di rete
Indirizzo IPv6	network ping6

Esempi

Il seguente comando crea una LIF e specifica i valori dell'indirizzo IP e della maschera di rete utilizzando `-address` e. `-netmask` parametri:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

Il seguente comando crea una LIF e assegna i valori dell'indirizzo IP e della maschera di rete dalla subnet specificata (denominata client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

Il seguente comando crea una LIF NVMe/FC e specifica `nvme-fc` protocollo dati:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

Modificare le LIF ONTAP

È possibile modificare una LIF modificando gli attributi, ad esempio il nodo principale o il nodo corrente, lo stato amministrativo, l'indirizzo IP, la netmask, la policy di failover, policy firewall e policy di servizio. È inoltre possibile modificare la famiglia di indirizzi di una LIF

da IPv4 a IPv6.

A proposito di questa attività

- Quando si modifica lo stato amministrativo di una LIF su inattivo, i blocchi NFSv4 in sospeso vengono mantenuti fino a quando lo stato amministrativo della LIF non viene riportato su UP.

  Per evitare conflitti di blocco che possono verificarsi quando altri LIF tentano di accedere ai file bloccati, è necessario spostare i client NFSv4 su un LIF diverso prima di impostare lo stato amministrativo su inattivo.

- Non è possibile modificare i protocolli dati utilizzati da un FC LIF. Tuttavia, è possibile modificare i servizi assegnati a una politica di servizio o la politica di servizio assegnata a una LIF IP.

  Per modificare i protocolli dati utilizzati da un LIF FC, è necessario eliminare e ricreare il LIF. Per apportare modifiche alla politica di servizio di un LIF IP, si verifica una breve interruzione durante l'esecuzione degli aggiornamenti.

- Non è possibile modificare il nodo principale o il nodo corrente di una LIF di gestione con ambito di nodo.
- Quando si utilizza una subnet per modificare l'indirizzo IP e il valore della maschera di rete per una LIF, viene assegnato un indirizzo IP dalla subnet specificata; se l'indirizzo IP precedente della LIF proviene da una subnet diversa, l'indirizzo IP viene restituito a tale subnet.
- Per modificare la famiglia di indirizzi di una LIF da IPv4 a IPv6, è necessario utilizzare la notazione con i due punti per l'indirizzo IPv6 e aggiungere un nuovo valore per `-netmask-length` parametro.
- Non è possibile modificare gli indirizzi IPv6 link-local configurati automaticamente.
- La modifica di una LIF che non ha una destinazione di failover valida per la LIF genera un messaggio di avviso.

  Se un LIF che non dispone di una destinazione di failover valida tenta di eseguire il failover, potrebbe verificarsi un'interruzione.

- A partire da ONTAP 9.5, è possibile modificare la politica di servizio associata a una LIF.

  In ONTAP 9.5, le policy di servizio sono supportate solo per i servizi peer di intercluster e BGP. In ONTAP 9.6, è possibile creare policy di servizio per diversi servizi di gestione e dati.

- A partire da ONTAP 9.11.1, il failover automatico di LIF iSCSI è disponibile sulle piattaforme ASA (All-Flash SAN Array).

  Per le LIF iSCSI pre-esistenti, ovvero le LIF create prima dell'upgrade alla versione 9.11.1 o successiva, è possibile modificare il criterio di failover in "Attiva il failover automatico della LIF iSCSI".

- ONTAP utilizza il Network Time Protocol (NTP) per sincronizzare l'ora nel cluster. Dopo aver modificato gli indirizzi IP LIF, potrebbe essere necessario aggiornare la configurazione NTP per evitare errori di sincronizzazione. Per maggiori informazioni, fare riferimento al"Knowledge Base NetApp : la sincronizzazione NTP non riesce dopo la modifica dell'IP LIF" .

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per modificare un'interfaccia di rete

Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare ⋮ **> Modifica** accanto all'interfaccia di rete che si desidera modificare.
3. Modificare una o più impostazioni dell'interfaccia di rete. Per ulteriori informazioni, vedere "Creare una LIF".
4. Salvare le modifiche.

CLI

Utilizzare la CLI per modificare una LIF

Fasi

1. Modificare gli attributi di una LIF utilizzando `network interface modify` comando.

   Nell'esempio seguente viene illustrato come modificare l'indirizzo IP e la maschera di rete dei dati LIF 2 utilizzando un indirizzo IP e il valore della maschera di rete della subnet client1_sub:

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   Nell'esempio seguente viene illustrato come modificare la politica di servizio di una LIF.

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

   Ulteriori informazioni su `network interface modify` nella "Riferimento al comando ONTAP".

2. Verificare che gli indirizzi IP siano raggiungibili.

Se si utilizza…	Quindi utilizzare…
Indirizzi IPv4	`network ping`
Indirizzi IPv6	`network ping6`

   Ulteriori informazioni su `network ping` nella "Riferimento al comando ONTAP".

Migrazione delle LIF ONTAP

Potrebbe essere necessario migrare un LIF a una porta diversa sullo stesso nodo o su un

nodo diverso all'interno del cluster, se la porta è guasta o richiede manutenzione. La migrazione di un LIF è simile al failover LIF, ma la migrazione LIF è un'operazione manuale, mentre il failover LIF è la migrazione automatica di un LIF in risposta a un errore di collegamento sulla porta di rete corrente del LIF.

Prima di iniziare

- È necessario che sia stato configurato un gruppo di failover per le LIF.
- Il nodo di destinazione e le porte devono essere operativi e devono poter accedere alla stessa rete della porta di origine.

A proposito di questa attività

- I LIF BGP risiedono sulla porta home e non possono essere migrati su altri nodi o porte.
- Prima di rimuovere la scheda NIC dal nodo, è necessario migrare i file LIF ospitati sulle porte appartenenti a una scheda NIC in altre porte del cluster.
- È necessario eseguire il comando per la migrazione di un LIF del cluster dal nodo in cui è ospitato il LIF del cluster.
- Una LIF con ambito di nodo, come LIF di gestione con ambito di nodo, LIF di cluster, LIF di intercluster, non può essere migrata a un nodo remoto.
- Quando si esegue la migrazione di un LIF NFSv4 tra nodi, si verifica un ritardo fino a 45 secondi prima che il LIF sia disponibile su una nuova porta.

  Per risolvere questo problema, utilizzare NFSv4.1 dove non si verificano ritardi.

- Puoi migrare LIF iSCSI su piattaforme ASA (All-Flash SAN Array) che eseguono ONTAP 9.11.1 o versioni successive.

  La migrazione delle LIF iSCSI è limitata alle porte sul nodo principale o sul partner ha.

- Se la tua piattaforma non è una piattaforma ASA (All-Flash SAN Array) che esegue ONTAP versione 9.11.1 o successiva, non puoi migrare le LIF iSCSI da un nodo a un altro nodo.

  Per aggirare questa restrizione, è necessario creare una LIF iSCSI sul nodo di destinazione. Ulteriori informazioni su "Creazione di LIF iSCSI".

- Se si desidera migrare una LIF (interfaccia di rete) per NFS su RDMA, assicurarsi che la porta di destinazione sia compatibile con RoCE. È necessario eseguire ONTAP 9.10.1 o versione successiva per migrare un file LIF con l'interfaccia CLI o ONTAP 9.12.1 per eseguire la migrazione utilizzando Gestione sistema. In System Manager, una volta selezionata la porta di destinazione compatibile con RoCE, selezionare la casella di controllo accanto a **Usa porte RoCE** per completare correttamente la migrazione. Scopri di più "Configurazione di LIF per NFS su RDMA".
- Le operazioni di offload delle copie VMware VAAI non vengono eseguite quando si esegue la migrazione della LIF di origine o di destinazione. Informazioni sulla funzione di off-load delle copie:
  - "Ambienti NFS"
  - "Ambienti SAN"

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per migrare un'interfaccia di rete

Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare ⋮ **> Migra** accanto all'interfaccia di rete che si desidera modificare.

   Per una LIF iSCSI, nella finestra di dialogo **Migrate Interface**, selezionare il nodo di destinazione e la porta del partner ha.

   Se vuoi migrare la LIF iSCSI in modo permanente, seleziona la casella di controllo. La LIF iSCSI deve essere offline prima di poter essere migrata in modo permanente. Inoltre, una volta migrata in modo permanente, una LIF iSCSI non può essere annullata. Non esiste alcuna opzione di revert.

3. Fare clic su **Migra**.
4. Salvare le modifiche.

CLI

Utilizzare la CLI per migrare una LIF

Fase

A seconda che si desideri migrare una LIF specifica o tutte le LIF, eseguire l'azione appropriata:

Se si desidera eseguire la migrazione…	Immettere il seguente comando…
Una LIF specifica	`network interface migrate`
Tutte le LIF di gestione dei dati e dei cluster su un nodo	`network interface migrate-all`
Tutte le LIF di una porta	`network interface migrate-all -node <node> -port <port>`

Nell'esempio seguente viene illustrato come migrare un LIF denominato `datalif1` Su SVM `vs0` alla porta `e0d` acceso `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

Nell'esempio seguente viene illustrato come migrare tutti i dati e le LIF di gestione del cluster dal nodo (locale) corrente:

```
network interface migrate-all -node local
```

Informazioni correlate

- "migrazione dell'interfaccia di rete"

Ripristina una LIF nella porta home dopo un failover di un nodo ONTAP o una migrazione delle porte

È possibile ripristinare la porta home di un LIF dopo il failover o la migrazione a una porta diversa manualmente o automaticamente. Se la porta home di un LIF specifico non è disponibile, LIF rimane sulla porta corrente e non viene ripristinata.

A proposito di questa attività

- Se si porta la porta home di un LIF in stato attivo prima di impostare l'opzione di revert automatico, il LIF non viene restituito alla porta home.
- Il LIF non viene ripristinato automaticamente a meno che il valore dell'opzione "auto-revert" non sia impostato su true.
- È necessario assicurarsi che l'opzione "auto-revert" (indirizzamento automatico) sia attivata per ripristinare le porte home dei file LIF.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per ripristinare un'interfaccia di rete alla porta home

Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare ⋮ **> Ripristina** accanto all'interfaccia di rete che si desidera modificare.
3. Selezionare **Ripristina** per ripristinare un'interfaccia di rete alla porta home.

CLI

Utilizzare l'interfaccia CLI per ripristinare la porta LIF home

Fase

Ripristinare manualmente o automaticamente la porta home di un LIF:

Se si desidera ripristinare la porta home di un LIF…	Quindi immettere il seguente comando…
Manualmente	`network interface revert -vserver vserver_name -lif lif_name`
Automaticamente	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

Ulteriori informazioni su `network interface` nella "Riferimento al comando ONTAP".

Recupera una LIF ONTAP configurata in modo errato

Non è possibile creare un cluster quando la rete del cluster è cablata a uno switch, ma

non tutte le porte configurate in Cluster IPSpace possono raggiungere le altre porte configurate in Cluster IPSpace.

A proposito di questa attività

In un cluster con switch, se un'interfaccia di rete del cluster (LIF) è configurata sulla porta errata o se una porta del cluster è collegata alla rete errata, il `cluster create` il comando può non riuscire e visualizzare il seguente errore:

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

Ulteriori informazioni su `cluster create` nella "Riferimento al comando ONTAP".

Il risultato del `network port show` comando potrebbe mostrare che diverse porte vengono aggiunte all'IPSpace del cluster perché sono connesse a una porta configurata con una LIF del cluster. Tuttavia, i risultati del `network port reachability show -detail` comando rivela quali porte non sono connesse tra loro.

Ulteriori informazioni su `network port show` nella "Riferimento al comando ONTAP".

Per eseguire il ripristino da una LIF del cluster configurata su una porta non raggiungibile con le altre porte configurate con le LIF del cluster, attenersi alla seguente procedura:

Fasi

1. Ripristinare la porta home del LIF del cluster alla porta corretta:

   ```
   network port modify -home-port
   ```

   Ulteriori informazioni su `network port modify` nella "Riferimento al comando ONTAP".

2. Rimuovere dal dominio di trasmissione del cluster le porte che non hanno LIF del cluster configurate:

   ```
   network port broadcast-domain remove-ports
   ```

   Ulteriori informazioni su `network port broadcast-domain remove-ports` nella "Riferimento al comando ONTAP".

3. Creare il cluster:

   ```
   cluster create
   ```

Risultato

Una volta completata la creazione del cluster, il sistema rileva la configurazione corretta e inserisce le porte nei domini di trasmissione corretti.

Informazioni correlate

- "visualizzazione della raggiungibilità delle porte di rete"

Eliminare le LIF ONTAP

È possibile eliminare un'interfaccia di rete (LIF) non più richiesta.

Prima di iniziare

I LIF da eliminare non devono essere in uso.

Fasi

1. Contrassegnare i file LIF che si desidera eliminare come amministrativamente bassi utilizzando il seguente comando:

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. Utilizzare `network interface delete` Comando per eliminare una o tutte le LIF:

Se si desidera eliminare…	Immettere il comando …
Una LIF specifica	`network interface delete -vserver vserver_name -lif lif_name`
Tutte le LIF	`network interface delete -vserver vserver_name -lif *`

   Ulteriori informazioni su `network interface delete` nella "Riferimento al comando ONTAP".

   Il seguente comando elimina LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Utilizzare `network interface show` Comando per confermare che la LIF è stata eliminata.

   Ulteriori informazioni su `network interface show` nella "Riferimento al comando ONTAP".

Configurare la LIF ONTAP Virtual IP (VIP)

Alcuni data center di prossima generazione utilizzano meccanismi di rete Layer-3 (IP) che richiedono il failover delle LIF nelle subnet. ONTAP supporta LIF dati IP virtuali (VIP) e il protocollo di routing associato, Border gateway Protocol (BGP), per soddisfare i requisiti di failover di queste reti di nuova generazione.

A proposito di questa attività

Una LIF dati VIP è una LIF che non fa parte di alcuna subnet ed è raggiungibile da tutte le porte che ospitano una LIF BGP nello stesso IPSpace. Una LIF dei dati VIP elimina la dipendenza di un host dalle singole interfacce di rete. Poiché più adattatori fisici trasportano il traffico dati, l'intero carico non viene concentrato su

un singolo adattatore e sulla subnet associata. L'esistenza di una LIF di dati VIP viene pubblicizzata ai router peer attraverso il protocollo di routing Border Gateway Protocol (BGP).

Le LIF dei dati VIP offrono i seguenti vantaggi:

- Portabilità LIF oltre un dominio o una subnet di trasmissione: I LIF dei dati VIP possono eseguire il failover su qualsiasi subnet della rete annunciando la posizione corrente di ciascun LIF dei dati VIP ai router tramite BGP.
- Throughput aggregato: Le LIF dei dati VIP possono supportare un throughput aggregato che supera la larghezza di banda di ogni singola porta, in quanto le LIF VIP possono inviare o ricevere dati da più subnet o porte contemporaneamente.

Impostazione del protocollo Border gateway (BGP)

Prima di creare LIF VIP, è necessario impostare BGP, il protocollo di routing utilizzato per annunciare l'esistenza di un LIF VIP ai router peer.

A partire da ONTAP 9.9,1, VIP fornisce l'automazione di routing predefinita opzionale utilizzando i gruppi peer BGP per semplificare la configurazione.

ONTAP offre un modo semplice per apprendere i percorsi predefiniti utilizzando i peer BGP come router next-hop quando il peer BGP si trova sulla stessa sottorete. Per utilizzare la funzione, impostare `-use-peer-as-next-hop` attributo a. `true`. Per impostazione predefinita, questo attributo è `false`.

Se sono stati configurati percorsi statici, questi sono ancora preferiti rispetto a questi percorsi automatici predefiniti.

Prima di iniziare

Il router peer deve essere configurato per accettare una connessione BGP da BGP LIF per il numero di sistema autonomo configurato (ASN).

> ONTAP non elabora gli annunci di route in entrata dal router; pertanto, è necessario configurare il router peer in modo che non invii aggiornamenti di route al cluster. In questo modo si riduce il tempo necessario alla comunicazione con il peer per diventare pienamente funzionale e l'utilizzo della memoria interna all'interno di ONTAP.

A proposito di questa attività

L'impostazione di BGP richiede la creazione di una configurazione BGP, la creazione di un BGP LIF e la creazione di un peer group BGP. ONTAP crea automaticamente una configurazione BGP predefinita con valori predefiniti quando viene creato il primo gruppo peer BGP su un nodo specifico.

Un BGP LIF viene utilizzato per stabilire sessioni TCP BGP con router peer. Per un router peer, un LIF BGP è il prossimo punto di accesso a un LIF VIP. Il failover è disattivato per BGP LIF. Un gruppo di peer BGP annuncia i percorsi VIP per tutte le SVM nell'IPSpace utilizzato dal gruppo di peer. L'IPSpace utilizzato dal gruppo peer viene ereditato dalla LIF BGP.

A partire da ONTAP 9.16,1, l'autenticazione MD5 è supportata sui gruppi di peer BGP per proteggere le sessioni BGP. Quando MD5 è abilitato, le sessioni BGP possono essere stabilite ed elaborate solo tra i peer autorizzati, evitando potenziali interruzioni della sessione da parte di un attore non autorizzato.

Ai comandi e `network bgp peer-group modify` sono stati aggiunti i seguenti campi `network bgp peer-group create`:

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

Questi parametri consentono di configurare un gruppo peer BGP con una firma MD5 per una maggiore protezione. I seguenti requisiti si applicano all'uso dell'autenticazione MD5:

- È possibile specificare il parametro solo `-md5-secret` quando il `-md5-enabled` parametro è impostato su `true`.
- Per abilitare l'autenticazione MD5 BGP, è necessario che IPsec sia attivato globalmente. La LIF BGP non è necessaria per avere una configurazione IPsec attiva. Fare riferimento alla "Configurare la crittografia IP Security (IPsec) over wire".
- NetApp consiglia di configurare MD5 sul router prima di configurarlo sul controller ONTAP.

A partire da ONTAP 9.9.1, sono stati aggiunti i seguenti campi:

- `-asn` Oppure `-peer-asn` (valore a 4 byte) l'attributo stesso non è nuovo, ma ora utilizza un intero a 4 byte.
- `-med`
- `-use-peer-as-next-hop`

È possibile effettuare selezioni di percorsi avanzate con il supporto MED (Multi-Exit discriminator) per la prioritizzazione dei percorsi. MED è un attributo facoltativo nel messaggio di aggiornamento BGP che indica ai router di selezionare il percorso migliore per il traffico. MED è un numero intero a 32 bit senza segno (0 - 4294967295); sono preferiti valori inferiori.

A partire da ONTAP 9.8, questi campi sono stati aggiunti a `network bgp peer-group` comando:

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

Questi attributi BGP consentono di configurare GLI attributi AS Path e community per il peer group BGP.

Sebbene ONTAP supporti gli attributi BGP indicati sopra, i router non devono rispettarli. NetApp consiglia di verificare gli attributi supportati dal router e di configurare i gruppi di peer BGP di conseguenza. Per ulteriori informazioni, consultare la documentazione BGP fornita dal router.

Fasi

1. Accedere al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Facoltativo: Creare una configurazione BGP o modificare la configurazione BGP predefinita del cluster eseguendo una delle seguenti operazioni:

   a. Creare una configurazione BGP:

```
network bgp config create -node {node_name | local} -asn <asn_number>
-holdtime
<hold_time> -routerid <router_id>
```

- Il `-routerid` parametro accetta un valore a 32 bit decimale puntato che deve essere univoco solo all'interno di un dominio AS. NetApp consiglia di utilizzare l'indirizzo IP v4 per la gestione dei nodi per `<router_id>` cui si garantisce l'unicità.
- Sebbene ONTAP BGP supporti numeri ASN a 32 bit, è supportata solo la notazione decimale standard. La notazione ASN tratteggiata, ad esempio 65000,1 invece di 4259840001 per un ASN privato, non è supportata.

Esempio con ASN a 2 byte:

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

Esempio con ASN a 4 byte:

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. Modificare la configurazione BGP predefinita:

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>` Specifica il numero ASN. A partire da ONTAP 9.8, ASN per BGP supporta un numero intero non negativo a 2 byte. Si tratta di un numero a 16 bit (da 1 a 65534 valori disponibili). A partire da ONTAP 9.9,1, ASN per BGP supporta un intero non negativo da 4 byte (da 1 a 4294967295). L'ASN predefinito è 65501. ASN 23456 è riservato per la creazione di sessioni ONTAP con peer che non annunciano funzionalità ASN a 4 byte.
- `<hold_time>` specifica il tempo di attesa in secondi. Il valore predefinito è 180 s.

ONTAP supporta solo un Global `<asn_number>`, , `<hold_time>` e `<router_id>`, anche se si configura BGP per IPSpace multipli. Il BGP e tutte le informazioni di routing IP sono completamente isolati all'interno di un IPSpace. Un IPSpace è equivalente a un'istanza di routing e inoltro virtuale (VRF).

3. Creare una LIF BGP per la SVM di sistema:

Per l'IPSpace predefinito, il nome della SVM è il nome del cluster. Per IPSpace aggiuntivi, il nome SVM è identico al nome IPSpace.

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

È possibile utilizzare `default-route-announce` Policy di servizio per BGP LIF o qualsiasi policy di servizio personalizzata che contenga il servizio "management-bgp".

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. Creare un peer group BGP utilizzato per stabilire sessioni BGP con i router peer remoti e configurare le informazioni di routing VIP pubblicizzate sui router peer:

   Esempio 1: Creazione di un gruppo di pari senza un percorso predefinito automatico

   In questo caso, l'amministratore deve creare un percorso statico al peer BGP.

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

   Esempio 2: Creazione di un gruppo di pari con un percorso predefinito automatico

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

Esempio 3: Creare un gruppo peer con MD5 attivato

a. Attiva IPSec:

```
security ipsec config modify -is-enabled true
```

b. Creare il gruppo di peer BGP con MD5 attivato:

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

Esempio utilizzando una chiave esagonale:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x746573742073656372657420
```

Esempio di utilizzo di una stringa:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

Dopo aver creato il gruppo di peer BGP, viene elencata una porta ethernet virtuale (che inizia con v0a..v0z,V1A...) quando si esegue il comando. `network port show` Il valore MTU di questa interfaccia è sempre riportato all'indirizzo 1500. La MTU effettiva utilizzata per il traffico deriva dalla porta fisica (BGP LIF), che viene determinata al momento dell'invio del traffico. Ulteriori informazioni su `network port show` nella "Riferimento al comando ONTAP".

Creare una LIF di dati IP (VIP) virtuale

L'esistenza di una LIF di dati VIP viene pubblicizzata ai router peer attraverso il protocollo di routing Border Gateway Protocol (BGP).

Prima di iniziare

- È necessario impostare il peer group BGP e attivare la sessione BGP per la SVM su cui deve essere creata la LIF.

- È necessario creare un percorso statico per il router BGP o qualsiasi altro router nella subnet della LIF BGP per qualsiasi traffico VIP in uscita per la SVM.
- È necessario attivare il routing multipath in modo che il traffico VIP in uscita possa utilizzare tutti i percorsi disponibili.

  Se il routing multipath non è attivato, tutto il traffico VIP in uscita viene gestito da una singola interfaccia.

Fasi

1. Creare una LIF dati VIP:

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role data
   -data-protocol
   {nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
   <ip_address> -is-vip true -failover-policy broadcast-domain-wide
   ```

   Se non si specifica la porta home con, viene selezionata automaticamente una porta VIP `network interface create` comando.

   Per impostazione predefinita, i dati VIP LIF appartengono al dominio di trasmissione creato dal sistema, denominato 'VIP', per ogni IPSpace. Non è possibile modificare il dominio di trasmissione VIP.

   Una LIF di dati VIP è raggiungibile simultaneamente su tutte le porte che ospitano una LIF BGP di un IPSpace. Se non è presente alcuna sessione BGP attiva per la SVM del VIP sul nodo locale, la LIF dei dati VIP esegue il failover alla porta VIP successiva sul nodo in cui è stata stabilita una sessione BGP per tale SVM.

2. Verificare che la sessione BGP si trovi nello stato up per la SVM dei dati VIP LIF:

   ```
   network bgp vserver-status show

   Node        Vserver  bgp status
           ----------  -------- ---------
           node1       vs1      up
   ```

   Se lo stato BGP è `down` Per la SVM su un nodo, la LIF dei dati VIP esegue il failover su un nodo diverso in cui lo stato BGP è attivo per la SVM. Se lo stato BGP è `down` Su tutti i nodi, la LIF dei dati VIP non può essere ospitata da nessuna parte e lo stato LIF è inattivo.

Comandi per la gestione del BGP

A partire da ONTAP 9.5, si utilizza `network bgp` Comandi per gestire le sessioni BGP in ONTAP.

Gestire la configurazione BGP

Se si desidera…	Utilizzare questo comando…
Creare una configurazione BGP	`network bgp config create`

Modificare la configurazione BGP	`network bgp config modify`
Eliminare la configurazione BGP	`network bgp config delete`
Visualizzare la configurazione BGP	`network bgp config show`
Visualizza lo stato BGP per la SVM della LIF VIP	`network bgp vserver-status show`

Gestire i valori predefiniti BGP

Se si desidera…	Utilizzare questo comando…
Modificare i valori predefiniti BGP	`network bgp defaults modify`
Visualizza i valori predefiniti BGP	`network bgp defaults show`

Gestire i peer group BGP

Se si desidera…	Utilizzare questo comando…
Creare un peer group BGP	`network bgp peer-group create`
Modificare un gruppo peer BGP	`network bgp peer-group modify`
Eliminare un gruppo peer BGP	`network bgp peer-group delete`
Visualizza le informazioni sui gruppi peer BGP	`network bgp peer-group show`
Rinominare un gruppo peer BGP	`network bgp peer-group rename`

Gestire i gruppi di pari BGP con MD5

A partire da ONTAP 9.16,1, è possibile attivare o disattivare l'autenticazione MD5 su un gruppo peer BGP esistente.

> Se si attiva o disattiva MD5 su un gruppo di peer BGP esistente, la connessione BGP viene terminata e ricreata per applicare le modifiche alla configurazione MD5.

Se si desidera…	Utilizzare questo comando…
Abilitare MD5 su un gruppo peer BGP esistente	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
Disattivare MD5 su un gruppo di peer BGP esistente	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

Informazioni correlate

- "Riferimento al comando ONTAP"
- "bgp di rete"

- "interfaccia di rete"
- "modifica della configurazione di sicurezza ipsec"

Informazioni sul copyright

Informazioni sul marchio commerciale